CLAIMS

What is claimed is:

1. A networked system for accessing information, comprising:

a first network station, representing a first network entity, configured to control access to information stored on a network for a third network entity, and to encrypt a first component message with a first crypto-key associated with the first network entity;

a second network station, representing a second network entity, configured to control access to the network by the third network entity, to encrypt a second component message with a second crypto-key, to combine the encrypted first and the encrypted second component messages, and to transmit the combined messages over the network; and

a third network station, representing the third network entity, configured to receive the transmitted combined messages and to further transmit the received combined messages over the network in order to obtain access to the stored information;

wherein the first network station is further configured to receive the further transmitted combined messages, to decrypt the encrypted first and the encrypted second component messages in the received further transmitted combined messages, and to control access by the third network station to the stored information based on the decrypted first and second component messages.

2. A networked system according to claim 1, wherein:

the first crypto-key is a symmetric crypto-key; and

the second crypto-key is a non-symmetric crypto-key.

3. A networked system according to claim 2, wherein:

the symmetric crypto-key is known only to the first network entity.

4. A networked system according to claim 2, wherein;

the non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

5. A networked system according to claim 1, wherein:

the first crypto-key is a first non-symmetric crypto-key; and

the second crypto-key is a second non-symmetric crypto-key, different than the first non-symmetric crypto-key.

6. A networked system according to claim 5, wherein:

the first non-symmetric crypto-key is a public crypto-key of a joint private-public crypto-key pair associated with the first network entity; and

the second non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

7. A networked system according to claim 1, wherein;

the first component message includes identity information associated with the third network entity, and integrity information which corresponds to the identity information; and

the second component message includes voucher information which indicates that the second network entity has authenticated the third network entity.

8. A networked system according to claim 1, further comprising:

a fourth network station, representing a fourth network entity, configured to encrypt a third component message with a third crypto-key, to initially combine the encrypted first and the encrypted third component messages, and to transmit the initially combined messages over the network;

wherein the second network station is further configured to receive the transmitted initially combined messages, to combine the encrypted first and the encrypted third component messages in the received initially combined messages with the encrypted second component message to create the combined messages;

wherein the first network station is further configured to decrypt the encrypted third component message in the received further transmitted combined messages, and to control access by the third network station to the stored information based also on the decrypted third component message.

9. A networked system according to claim 8, wherein:

the first component message includes identity information associated with the third network entity, and integrity information which corresponds to the identity information;

the second component message includes voucher information which indicates that the second network entity has authenticated the third network entity; and

the third component message includes relationship information which indicates that the identity and the integrity information was received by the fourth network entity from the first network entity and transmitted by the fourth network entity to the second network entity.

10. A networked system according to claim 8, wherein:

the first crypto-key is a symmetric crypto-key;

the second crypto-key is a non-symmetric crypto-key; and

the third crypto-key is a non-symmetric crypto-key.

11. A networked system according to claim 1, wherein:

the second component message further includes a timestamp corresponding to a time at which the combined messages are transmitted by the second network station.

12. A networked system according to claim 1, wherein:

the first network station is further configured to combine the encrypted first component message with a network address for the stored information;

the second network station is further configured to combine the combined encrypted first component message and the network address with the encrypted second component message to create the combined messages; and

the first network station is further configured to control access by the third network station to the stored information based on the network address and the decrypted first and second component messages.

13. A networked system according to claim 1, wherein:

the second network station transmits the combined message in response to a received request;

the first network station encrypts the first component message prior to receipt of the request by the second network station; and

the second network station encrypts the second component message and combines the encrypted first and the encrypted second component messages after receipt of the request by the second network station.

14. A method of creating an electronic message for transmission over a network, comprising the steps of:

encrypting a first component with a first crypto-key, associated with a first network entity, such that the encrypted first component can be decrypted by only the first network entity;

encrypting a second component with a second crypto-key, associated with a second network entity, such that the encrypted second component can be decrypted by the first network station; and

transmitting the encrypted first component and the encrypted second component as a combined message.

15. A method according to claim 14, wherein:

the first crypto-key is a symmetric crypto-key; and

the second crypto-key is a non-symmetric crypto-key.

16. A method according to claim 15, wherein:

the symmetric crypto-key is known only to the first network entity; and

the non-symmetric crypto-key is known only to the second network entity.

17. A method according to claim 15, wherein;

the non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

18. A method according to claim 14, wherein:

the first crypto-key is a first non-symmetric crypto-key; and

the second crypto-key is a second non-symmetric crypto-key.

19. A method according to claim 18, wherein:

the first non-symmetric crypto-key is a public crypto-key of a joint private-public crypto-key pair associated with the first network entity; and

the second non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

20. A method according to claim 14, further comprising the steps of:

encrypting a third component with a third crypto-key, associated with a third network entity, such that the encrypted third component can be decrypted by the first network entity; and

transmitting the encrypted third component with the encrypted first and the encrypted second components as the combined message.

21. A method according to claim 20, wherein:

the first crypto-key is a symmetric crypto-key;

the second crypto-key is a first non-symmetric crypto-key; and

the third crypto-key is a second non-symmetric crypto-key.

22. A method according to claim 20, wherein:

the first component includes identity information associated with a fourth network entity and integrity information corresponding to the identity information;

the second component includes relationship information which indicates that the identity and the integrity information were received by the second network entity from the first network entity and transmitted by the second network entity to the third network entity; and

the third component includes voucher information which indicates that the third network entity authenticated the fourth network entity.

23. A method according to claim 20, wherein:

the third component further includes a timestamp corresponding to a time at which the combined message is transmitted to the fourth network entity.

24. A method according to claim 20, further comprising the step of:

transmitting the encrypted first, the encrypted second and the encrypted third components with a network address as the combined message.

25. A method according to claim 14, wherein:

the combined message is transmitted responsive to a received request;

the first component is encrypted prior to receipt of the request; and

the second component is encrypted after receipt of the request.

26. An electronic message, comprising:

a first component created by a first network entity and encrypted with a first crypto-key, associated with the first network entity, such that the encrypted first component can be decrypted by only the first entity; and

a second component created by a second network entity, and encrypted with a second crypto-key, such that the encrypted second component can be decrypted by the first network entity.

27. An electronic message according to claim 26, wherein:

the first crypto-key is a symmetric crypto-key known only to the first network entity; and

the second crypto-key is a non-symmetric crypto-key.

28. An electronic message according to claim 27, wherein;

the non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

29. An electronic message according to claim 26, wherein:

the first crypto-key is a first non-symmetric crypto-key; and

the second crypto-key is a second non-symmetric crypto-key.

30. An electronic message according to claim 29, wherein:

the first non-symmetric crypto-key is a public crypto-key of a joint private-public crypto-key pair associated with the first network entity; and

the second non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second network entity.

31. An electronic message according to claim 26, further comprising:

a third component created by a third network entity and encrypted with a third crypto-key, associated with the third network entity, such that the encrypted third component can be decrypted by the first network entity.

32. An electronic message according to claim 31, wherein:

the first component includes identity information associated with a fourth network entity, and integrity information corresponding to the identity information;

the second component includes relationship information which indicates that the identity and the integrity information were received by the second network entity from the first network entity and transmitted by the second network entity to the third network entity; and

the third component includes voucher information which indicates that the third network entity has authenticated the fourth network entity.

33. An electronic message according to claim 32, wherein:

the integrity information includes a hash of the identity information.

34. An electronic message according to claim 32, wherein:

the third component further includes a timestamp corresponding to a time at which the electronic message is transmitted by the third network entity to the fourth network entity.

35. An electronic message according to claim 26, wherein:

the first component includes identity information associated with a third network entity;

the second component includes voucher information which indicates that the second network entity has authenticated the third network entity.

36. An electronic message according to claim 35, wherein:

the second component further includes a timestamp corresponding to a time at which the electronic message is transmitted by the second network entity to the third network entity.

37. An electronic message according to claim 26, wherein:

the first network entity controls access to information available on a network; and

the second entity controls access to other network entities.

38. An electronic message according to claim 26, wherein the first component includes an identification of information stored on a network, and further comprising:

a network address at which the identified stored information can be accessed.

39. An electronic message, comprising:

a first component encrypted with only a symmetric crypto-key; and

a second component, different than the first component, encrypted with only a non-symmetric crypto-key.

40. An electronic message according to claim 39, wherein:

the symmetric crypto-key is associated with a first entity; and

the non-symmetric crypto-key is associated with a second entity.

41. An electronic message according to claim 40, wherein:

the symmetric crypto-key is known only to the first entity.

42. An electronic message according to claim 40, wherein;

the non-symmetric crypto-key is a private crypto-key of a joint private-public crypto-key pair associated with the second entity.

43. An extended network universal resource locator, comprising:

a first component including a network address at which stored information can be accessed on a network;

a second component including identity information associated with a first network entity and an integrity value corresponding to the identity information, the second component being encrypted with a first crypto-key of a second network entity; and

a third component including voucher information indicating that a third network entity has authenticated the first network entity and that transmission of the extended network universal resource locator by the third network entity to the first network

entity occurred at a particular time, the third component being encrypted with a second crypto-key of the third network entity.

44. An extended universal resource locator according to claim 43, further comprising:

a fourth component including relationship information indicating that the encrypted second component was received by a fourth network entity from the second network entity and transmitted by the fourth network entity to the third network entity, the fourth component being encrypted with a third crypto-key of the fourth network entity.

45. An extended universal resource locator according to claim 44, wherein:

the first crypto-key is a symmetric crypto-key known only to the second network entity;

the second crypto-key is a first non-symmetric crypto-key associated with the third network entity; and

the third crypto-key is a second non-symmetric crypto-key associated with the fourth network entity.

46. An extended universal resource locator according to claim 45, wherein;

the first non-symmetric crypto-key is one of a private crypto-key and a public crypto-key of a joint private-public crypto-key pair associated with the third network entity; and

the second non-symmetric crypto-key is one of a private crypto-key and a public crypto-key of a joint private-public crypto-key pair associated with the fourth network entity.

47. An extended universal resource locator according to claim 44, wherein:

the stored information is detailed bill information;

the network address is an Internet URL;

the identity information includes an identification of the stored information and an account number associated with the first network entity;

the integrity value is a hash of the identity information; and

the transmission time information is a timestamp.

48. An extended universal resource locator according to claim 44, wherein:

the second network entity controls access to the stored information;

the fourth network entity controls access to other information which is transmitted with the extended network universal resource locator by the third network entity to the first network entity; and

the third network entity controls access by the first network entity to other network entities.

49. An extended universal resource locator according to claim 48, wherein:

the stored information is detailed bill information associated with the first entity; and

the other information is summary bill information associated with the first network entity.